Configure remote authentication through TACACS+

Published: 2018-11-09

The ExtraHop appliance supports Terminal Access Controller Access-Control System Plus (TACACS+) for remote authentication and authorization.

Ensure that each user to be remotely authorized has the ExtraHop service configured on the TACACS+ server before beginning this procedure.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **TACACS+**, and then click **Continue**.
4. On the Add TACACS+ Server page, type the following information:

   • Host**:** The hostname or IP address of the TACACS+ server. Make sure that the DNS of the ExtraHop appliance is properly configured if you are entering a hostname.

   • Secret**:** The shared secret between the ExtraHop appliance and the TACACS+ server. Contact your TACACS+ administrator to obtain the shared secret.

   • Timeout**:** The amount of time in seconds that the ExtraHop appliance waits for a response from the TACACS+ server before attempting to connect again.
5. Click **Add Server**.
6. Optional: Add additional servers as needed.
7. Click **Save and Finish**.
8. From the Permission assignment options drop-down list, choose one of the following options:
   - **Obtain privileges level from remote server**

     This option allows remote users to obtain privilege levels from the remote server. You must also configure permissions on the TACACS+ server.
   - **Remote users have full write access**

     This option allows remote users to have full write access to the ExtraHop Web UI.
   - **Remote users have full read-only access**

     This option allows remote users to have read-only permissions to the ExtraHop Web UI.

     Note: You can add read-write privileges on a per-user basis later through the Users page in the Admin UI.
   - **Remote users can view connected appliances**

     This option, which only appears on the Command appliance, allows remote users to log into the Admin UI on the Command appliance and view any connected Discover, Explore, and Trace appliances.
9. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packets only**
   - **Packets and session keys**
10. Click **Save and Finish**.
11. Click **Done**.

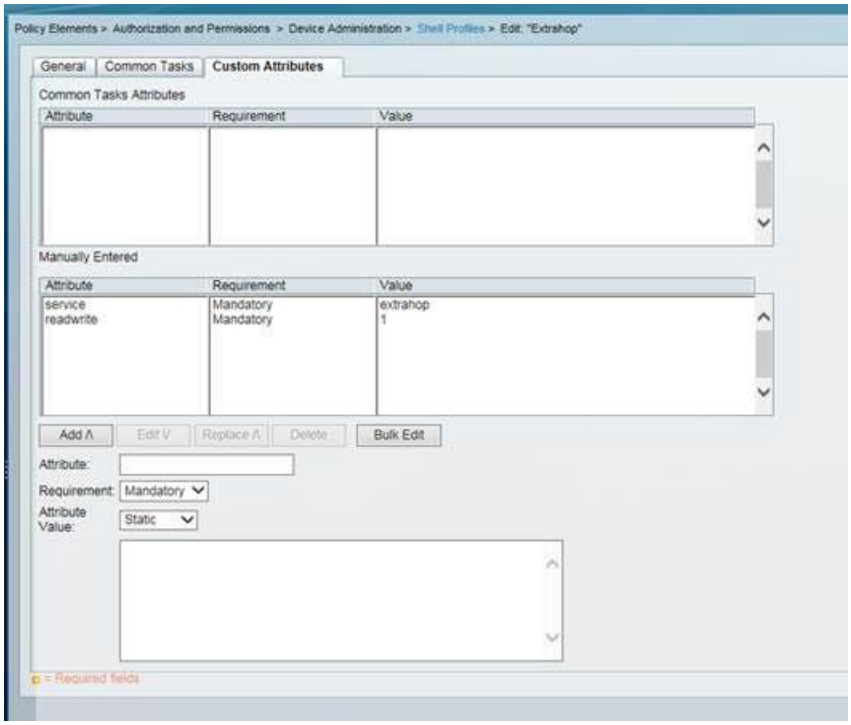
© 2018 ExtraHop Networks, Inc. All rights reserved.

Configure the TACACS+ server

In addition to configuring remote authentication on your ExtraHop appliance, you must configure your TACACS+ server with two attributes, one for the ExtraHop service and one for the permission level. If you have a Trace appliance, you can optionally add a third attribute for packet capture and session key logging.

1. Log into your TACACS+ server and navigate to the shell profile for your ExtraHop configuration.
2. For the first attribute, add `service`.
3. For the first value, add `extrahop`.
4. For the second attribute, add the permission level, such as `readwrite`.
5. For the second value, add `1`.

   For example, the following figure shows the `extrahop` attribute and a permission level of `readwrite`.



   Here is a list of available permission attributes, values, and descriptions:

   - `setup = 1`, which allows the user to create and modify all objects and settings on the ExtraHop Web UI and Admin UI
   - `readwrite = 1`, which allows the user to create and modify all objects and settings on the ExtraHop Web UI
   - `limited = 1`, which allows the user to create, modify, and share dashboards
   - `readonly = 1`, which allows the user to view objects in the ExtraHop Web UI
   - `personal = 1`, which allows the user to create dashboards for themselves and modify any dashboards that have been shared with them
   - `limited_metrics = 1`, which allows the user to view shared dashboards
6. Optional: If you have a Trace appliance, add a third attribute to allow users to download packet captures or packet captures with associated session keys.

   Here is a list of the available packet capture attributes and values:

   - `packetsfull = 1`, which allows users with any permission level to view and download packets
   - `packetsfullwithkeys = 1`, which allows users with any permission level to view and download packets and associated session keys stored on the Trace appliance